LastPass by LogMeIn

Solution Overview

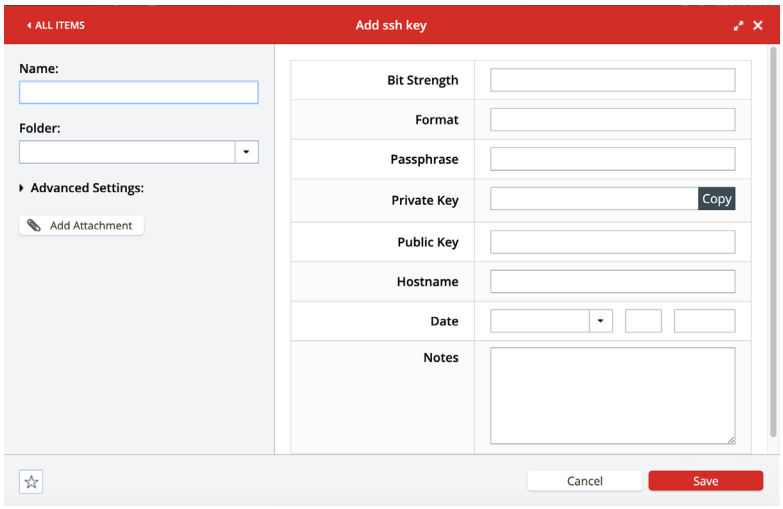
How LastPass Can Help Secure Privileged Accounts

Privileged accounts contain your company's most sensitive information. It can be a challenge to securely delegate access to employees, vendors, contractors, or others.

With LastPass, you can authorize, secure and manage access to your privileged accounts from one centralized dashboard. In addition to storing app and web-based logins, items such as server or Wi-Fi credentials can also be stored and shared with others.

When it comes to securing privileged accounts, LastPass allows you to:

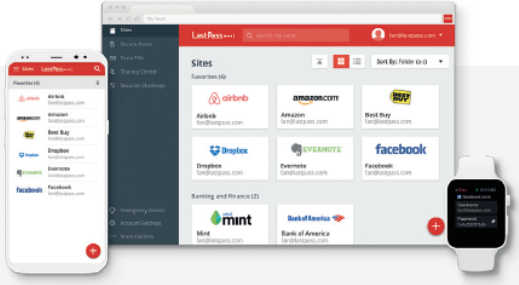
- Maintain an encrypted password vault for access from any device, app, Command Line Interface, or API
- Combine all privileged accounts in Shared Folders for secure access among team members, while maintaining accountability at the individual level
- Use the Command Line Interface to create custom scripts to retrieve privileged keys and rotate passwords, without sharing the password
- Store and share non web-based account information, such as server or router credentials, SSH keys, SSID, and more
- Maintain your company's security policies and process with the ability to create your own API with LastPass to control and manage privileged keys
- Ensure data is kept secure with encryption and decryption at the device level, keeping data secret from unauthorized users, including LastPass



When it comes to improving password security, don't stop at privileged accounts. LastPass Enterprise protects every access point through an all-in-one single sign-on and password manager solution. IT can leverage 100+ custom policies, automated user management, security reporting and more to safeguard every password-protected entry point, while simplifying everyday access for employees. Employees have simple access to IT-supported apps through single sign-on and can store all other apps in their password vault. With LastPass Enterprise, IT gains critical visibility into access across the business, no matter the entry point.

These features deliver the control IT needs and the convenience users expect:

Central admin control	The admin dashboard gives IT a unified view of access across the business and centralizes management of users, policies, reporting and more.
Adaptive multifactor authentication	Eliminate passwords while increasing security by combining biometrics and contextual factors to adapt authentication requirements to different situations.
Single sign-on	With a catalog of 1200+ pre-integrated apps, it's simple for IT to make critical business tools accessible to employees in one convenient portal.
Password vaulting	For the apps IT doesn't know about, LastPass Identity offers password management features that capture, store and fill credentials for any web-based login.
User directory integrations	Automate onboarding and offboarding, group management and more with AD, Azure AD, Okta, OneLogin or a custom API.
100+ security policies	Enforce best practices and control password behavior across the business.
Detailed security reports	Tie actions to individuals with automated, detailed reporting that helps your business maintain compliance.
Secure password sharing	Give teams a flexible, safe way to share access to apps without sacrificing accountability or security.



Visit www.lastpass.com/products/identity *to learn more*

©2019 LogMeIn, Inc. All rights reserved.